# Conceptual TIC Architecture:

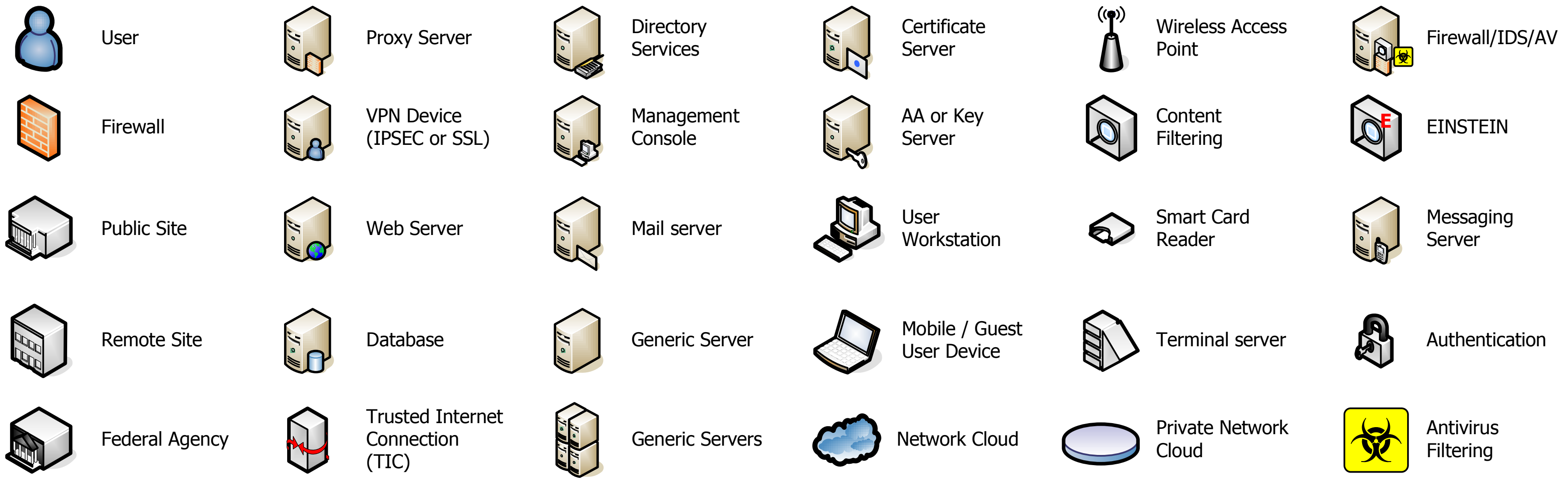
**Revision 1.0**
**09.2008**

## Conceptual TIC Architecture:
# Terms and Symbols

**External Connection:** A physical or logical connection between information systems, networks, or components of information systems & networks that are, respectively, inside and outside of specific Department or Agency's (D/A) certification and accreditation (C&A) boundaries established by the D/A, for which the D/A has no direct control over the application of required security controls or the assessment of security control effectiveness on the outside information system, network, or components of information systems & networks; or the D/A, notwithstanding any direct or indirect control over the application of required security controls or the assessment of security control effectiveness, has specific reason to believe that the external system has a substantially reduced set of security controls or an increased threat posture relative to the internal system.

**Trusted Internet Connection (TIC):** The physical location agencies utilize to meet the TIC Initiative objective to reduce and consolidate external connections which are securely managed and monitored with a consistent set of security controls. TICs may be built and managed by an agency for their own use, or TIC services may be procured through a 3rd party provider.

**Trusted Internet Connection Access Provider (TICAP):** The entity responsible for managing a TIC.



User
Proxy Server
Directory Services
Certificate Server
Wireless Access Point
Firewall/IDS/AV

Firewall
VPN Device (IPSEC or SSL)
Management Console
AA or Key Server
Content Filtering
EINSTEIN

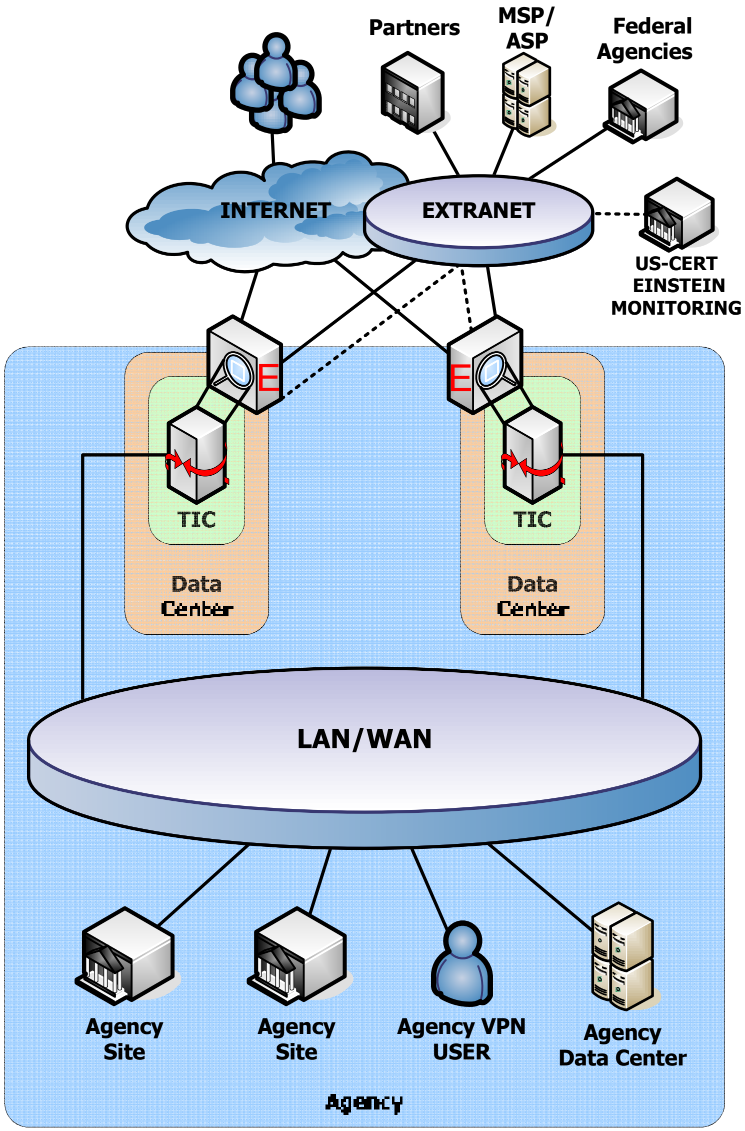
Public Site
Web Server
Mail server
User Workstation
Smart Card Reader
Messaging Server

Remote Site
Database
Generic Server
Mobile / Guest User Device
Terminal server
Authentication

Federal Agency
Trusted Internet Connection (TIC)
Generic Servers
Network Cloud
Private Network Cloud
Antivirus Filtering

**Note:** Throughout this document symbols are logical, not physical, representations of equipment and services.

# Conceptual TIC Architecture: TIC Overview



## Concepts and Strategies

❑ EINSTEIN deployed at "TICs" and monitoring all traffic that passes through the TIC to/from Internet or Extranet locations.

❑ The following types of connections will NOT typically be considered "external connections" and would not be required to, but could at the D/A's discretion, route through a TIC:

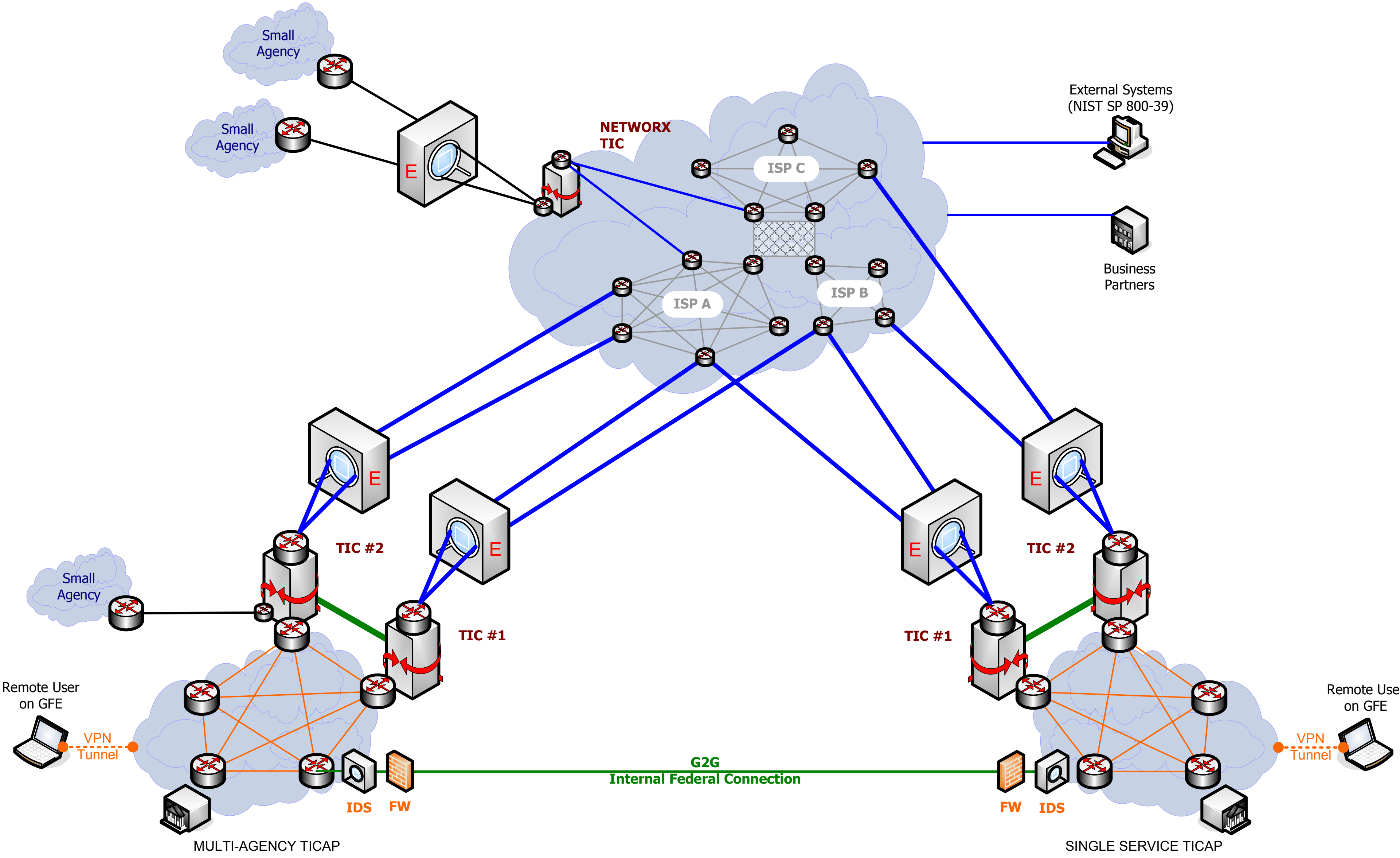
- Dedicated secure point-to-point connections that link information systems, networks, or components of information and systems and networks of a single D/A under a single certification and accreditation authority, provided that the connections do not access the globally-addressable internet; or
- Connections established through virtual private network technology utilizing security controls that at a minimum are compliant with FIPS 140-2 and NIST 800-53 coupled with D/A auditing and monitoring of the connections.

❑ Interconnections among D/As may be considered "internal connections" when all D/As involved in the interconnect are fully behind TICs and the following five criteria are met:

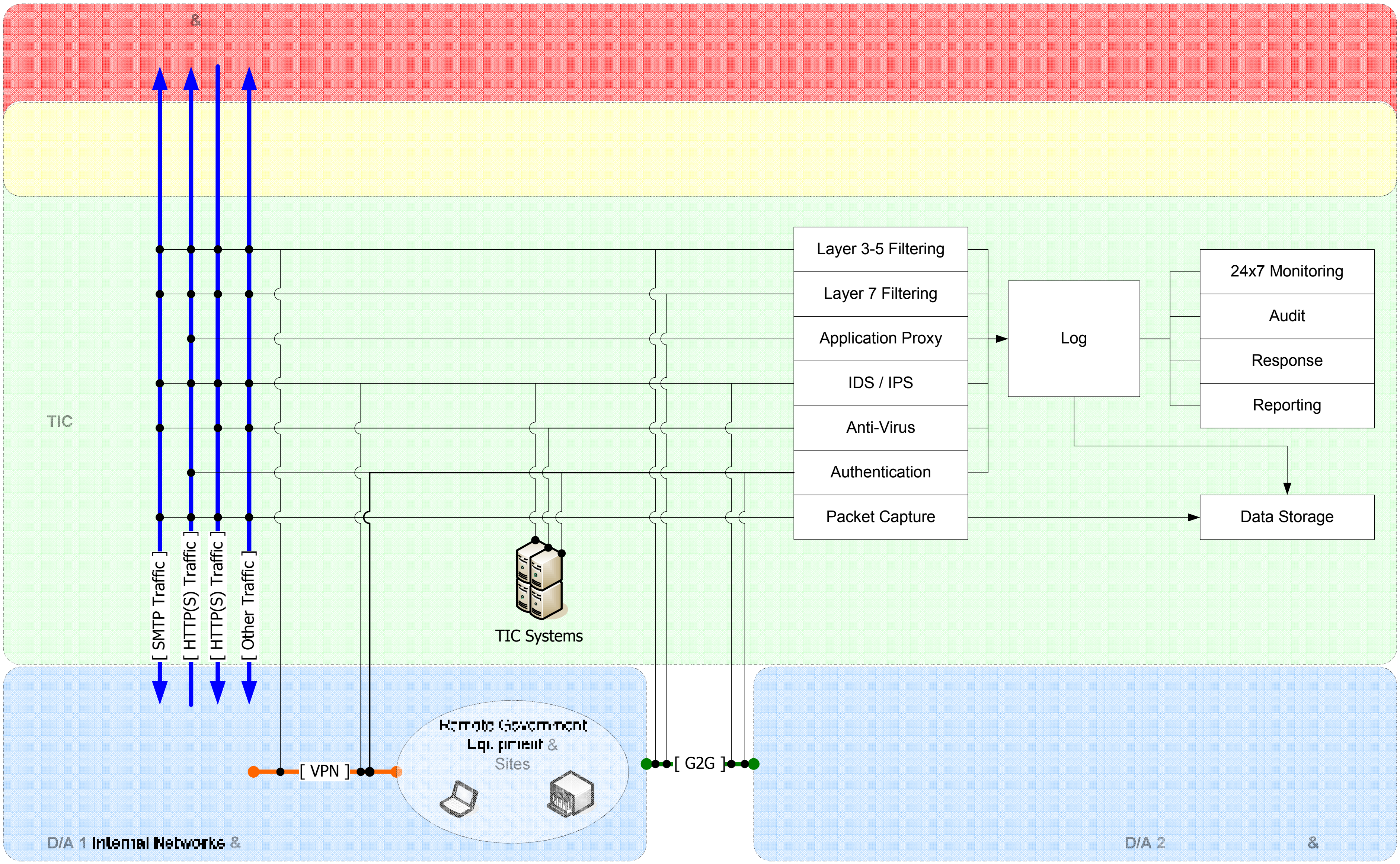
- All of the D/As external connections route through a TIC, and;
- All D/As monitor the connection at the point of ingress into their C&A boundary using COTS/GOTS IDS software, and;
- All D/As perform packet screening to ensure that only authorized traffic is permitted to flow between the interconnected D/As, and;
- All D/As maintain the capability to suspend/temporarily deactivate the connection in the event that suspicious activity is detected.

## Conceptual TIC Architecture:

# TIC Enterprise Level Architecture



| INTERNET Traffic | InterTIC & InterAgency traffic | Intra-Agency Traffic | TIC Client Traffic | Forbidden Connection |
|---|---|---|---|---|
| 🟦 | 🟩 | 🟧 | ⬛ | 🟥 |



INTERNET Traffic

InterTIC & InterAgency traffic

Intra-Agency Traffic

TIC Client Traffic

Forbidden Connection

**TIC Network & Data Controls:**

# Conceptual Model for Network Controls and Trust Relationships

## Model Description

- ❑ The Network is organized logically around three levels (zones) of trust. Each level of trust reflects specific controls applied to the systems and networks residing within. The default three levels of trust are:
  - **External Zone**: Information systems or components of information systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
  - **Internal Zone**: Information systems or components of information systems that are within the accreditation boundary established by the organization and for which the organization typically has direct control over the application of required security controls or the assessment of security control effectiveness.
  - **TIC Zone:** Border between an organizations Internal infrastructure (users, systems, data) and External resources. Serves as the termination point for external connections and utilizes a standard set of security controls to monitor, authenticate and filter data flows that enter/exit the TIC.
- ❑ Communications are denied by default when traveling from less to more trusted systems and allowed by default when traveling from more to less trusted systems.
- ❑ The TIC will be comprised of security controls and DMZ networks defined according to function, data sensitivity and user constituency served. Direct data flows (unfiltered, unmonitored) between DMZ networks in the TIC will not be allowed.
- ❑ With appropriate hardware, security software and authentication encrypted VPN sessions originating on External networks (e.g., remote office or mobile employee) will be allowed and considered logical extensions of the agencies Internal network.
- ❑ EINSTEIN deployed and monitoring all External traffic that enters or exits the TIC (both Internet and Extranet traffic); EINSTEIN sensors utilize an isolated, out of band extranet connection to communicate with US-CERT resources and are monitored by US-CERT.
- ❑ Firewalls shall perform Stateful Inspection of all traffic that enters/exits the TIC with Deep Packet Inspection or Application Proxy capabilities preferred.
- ❑ Traffic known to be malicious or counter to agency policy will not be allowed to pass through a TIC
- ❑ Internal users will utilize a Web Proxy Server for http, https access to external sites.
  - The content of web sessions will be filtered based on destination URL or IP address, text content of web pages, and/or the presence of active content (e.g. Java, Active X).
  - Traffic that does not utilize a proxy will require an exemption / prior approval
- ❑ No Direct (unfiltered, unmonitored) connections between External and Internal systems

## Design Considerations and Standards

- Federal Enterprise Architecture (OMB)
- Federal Laws and Regulations
  GLB, HIPPA, SBO, HSPDs
- ISO 17799
- Agency Policies
- Generally Accepted Best Practices
- NIST Special Publications:
  800-27A, 32, 33, 44-48, 53

### TIC Network & Data Controls:

# Conceptual Model for Network Controls and Trust Relationships

## Model Description (continued)

**HTTP/HTTPS, SMTP Traffic Proxy & Monitoring and Anti Virus & Content Filtering**

□ Monitor unencrypted inbound/outbound SMTP messages and filter messages based on, but not limited to: unauthorized/known bad mail source or destination, suspicious text patterns, unauthorized file attachment type, message size, unsigned active content
□ Malware scan unencrypted inbound/outbound SMTP messages and block infected messages
□ SPAM filter inbound/outbound SMTP Messages
□ Block inbound/outbound traffic to/from specified (e.g. known malicious) IP or URL
□ Block inbound/outbound traffic based on protocol (e.g. ftp, IM)
□ User web sessions (http, https) only via an approved proxy
□ Any non-proxied traffic shall require prior approval
□ Filter the content of all proxied web sessions. The outbound web proxy server will filter based on destination URL or IP address, text content of web pages, and/or the presence of active content (e.g. Java, Active X).

□ Use the concept of "Defense in depth" to guide security architecture
□ Use multiple layers of controls between "external" devices/environments and "internal" applications, devices and data
□ Use non-technology controls (physical, management, etc) in conjunction with technology controls where appropriate
□ Uses a combination of network- and application-layer technology controls
□ Bases Network Security on a Conceptual "Model of Trust"
□ Simplified Network Data Flow Policy
□ Network access control systems will be configured to enforce a bi-directional policy of "default deny" between agency systems and external resources, but elsewhere will be configured to "default allow" data flow from more trusted to less trusted and default-deny from less trusted to more trusted environments.
□ Strong authentication mechanisms where appropriate
  - Two-factor or certificate-based authentication for TIC systems administration access and for remote VPN access
  - Within other applications on an  needed basis

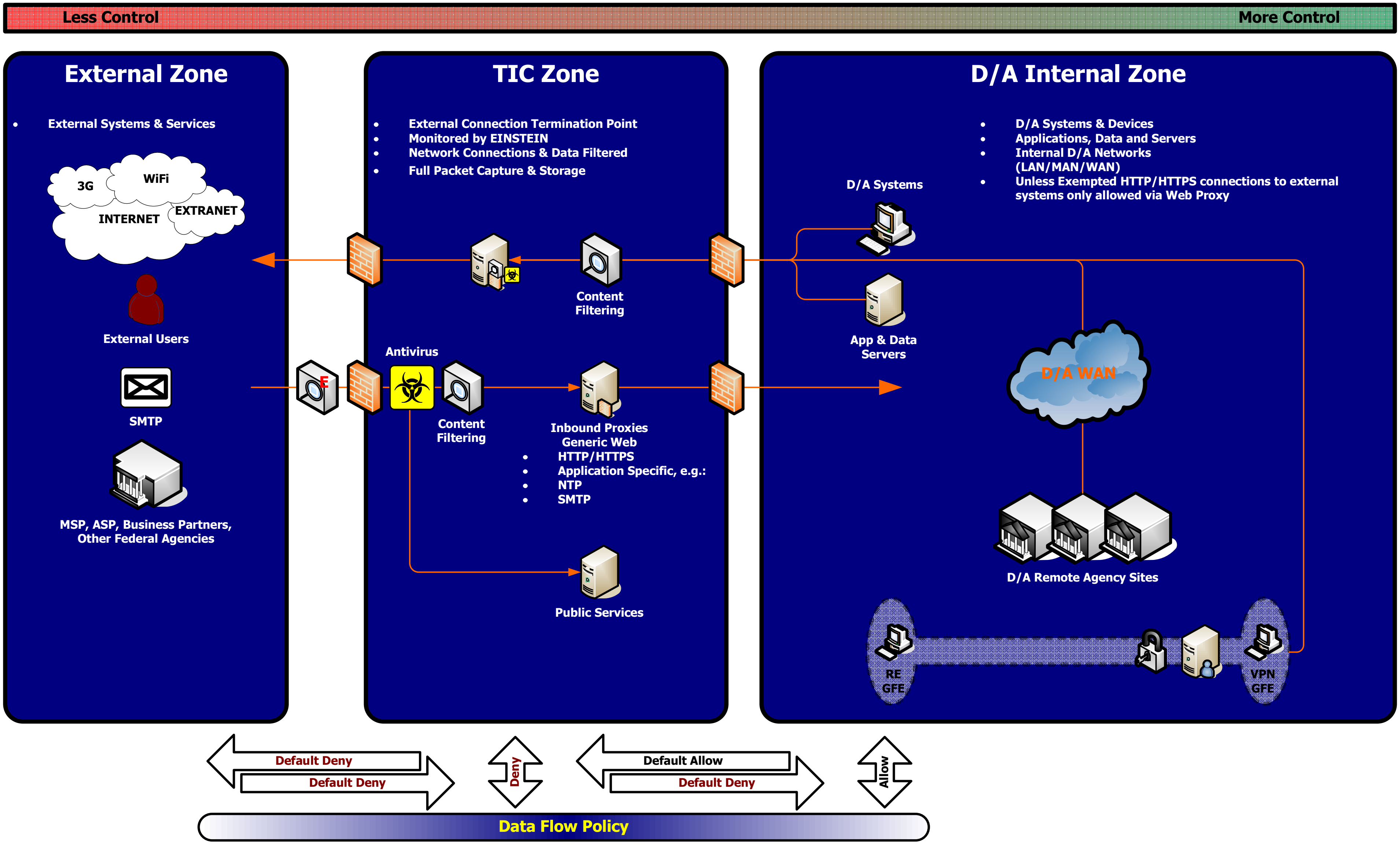
□ Utilize Virus Defense with multiple overlapping layers

## Design Considerations and Standards

- Federal Enterprise Architecture (OMB)
- Federal Laws and Regulations
  GLB, HIPPA, SBO, HSPDs
- ISO 17799
- Agency Policies
- Generally Accepted Best Practices
- NIST Special Publications:
  800-27A, 32, 33, 44-48, 53

## Network & Data Controls:

# Conceptual Model for TIC Network Controls and Trust Relationships



**External Zone**

- External Systems & Services

**TIC Zone**

- External Connection Termination Point
- Monitored by EINSTEIN
- Network Connections & Data Filtered
- Full Packet Capture & Storage

**D/A Internal Zone**

- D/A Systems & Devices
- Applications, Data and Servers
- Internal D/A Networks (LAN/MAN/WAN)
- Unless Exempted HTTP/HTTPS connections to external systems only allowed via Web Proxy

⇔ Recommended **Inter-zone** Data Flow Policy

⇕ Recommended **Intra-zone** Data Flow Policy